PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-245605
(43)Date of publication of application : 19.09.1995

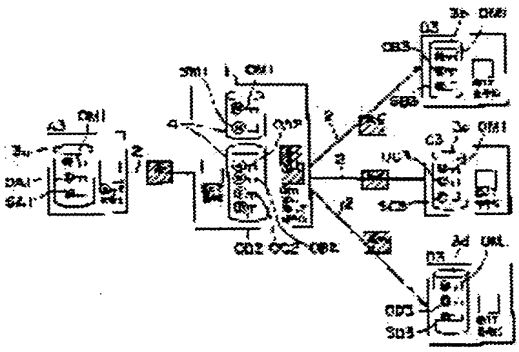
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G09C 1/00

(21)Application number : 06-033647
(22)Date of filing : 03.03.1994

(71)Applicant : FUJITSU LTD
(72)Inventor : KURODA YASUTSUGU
KIKUCHI HIROAKI

(54) CIPHERING INFORMATION REPEATER, SUBSCRIBER TERMINAL EQUIPMENT CONNECTING THERETO AND CIPHERING COMMUNICATION METHOD

(57)Abstract:
PURPOSE: To minimize secret information to be managed by each member and to allow the method to flexibly cope with subscription / withdrawal of a member by allowing the ciphering information repeater to act like a management center of a secret key.
CONSTITUTION: A subscriber caller terminal equipment A3 ciphers information by using an open key OM 1 and sends the ciphered information to a communication line 2, a ciphering information repeater 1 receives the information and decodes the information into a plain text with a secret key SM 1. Then the repeater 1 ciphers again the plain text information with an open key OB 2 of a subscriber terminal equipment B and sends the ciphered information to the line 2. A terminal equipment B3 receives the information and decodes the information into a plain text with its own secret key SB 3. In the case of re-ciphering by the repeater 1, the repeater 1 uses open keys OC2, OD2 similarly to cipher the information and sends the ciphered information to terminal equipments C3, D3, which respectively decode the information into a plain text by using their own respective secret keys SC3, SD4. The repeater 1 centralizingly manages the open key information of each subscriber in this way and each subscriber has only to combine the common open key OM1 with its own open key and secret key. Thus, a subscriber's subscription/withdrawal is implemented by having only to rewrite data of the repeater 1.



LEGAL STATUS

[Date of request for examination] 20.04.2000
[Date of sending the examiner's decision of rejection] 11.12.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－245605

(43)公開日　平成７年(1995)９月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9364－5Ｌ		
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願平6－33647

(22)出願日　平成６年(1994)３月３日

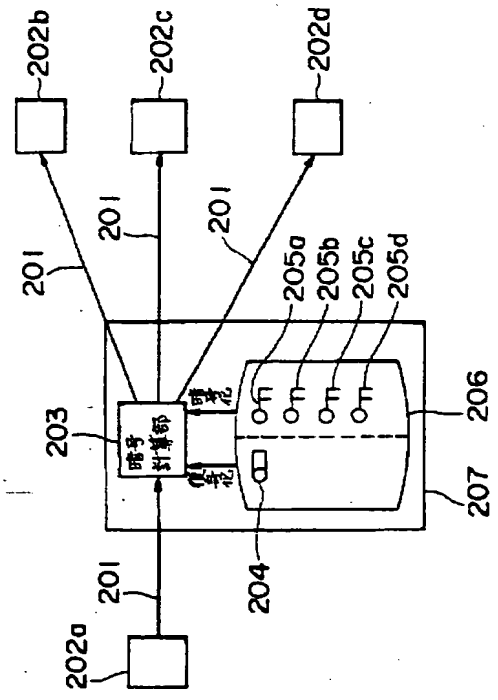
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　菊池　浩明
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　遠山　勉　（外１名）

(54)【発明の名称】　暗号化情報中継装置とそれに接続される加入者端末装置ならびに暗号通信方法

(57)【要約】

【目的】　メンバの加入・脱退にも柔軟に対応できる同報暗号通信システムを提供する。

【構成】　通信回線で接続された複数の加入者間で情報の送受信を行うシステムであって、前記発信加入者からの受信した暗号化情報の復号化、または受信加入者に送信する情報の暗号化を行う暗号計算部と、前記復号化するための共通秘密鍵と、各加入者に対応した暗号化を行うための各加入者毎の個別鍵とを格納した鍵格納部とを有する暗号化情報中継装置とし、各加入者の端末では保持すべき秘密情報を最小限とし、情報の盗聴や情報発信者のなりすましを防止できるようにした。



【特許請求の範囲】
【請求項１】　通信回線（２０１）で接続された複数の加入者間（２０２ａ，２０２ｂ，２０２ｃ，２０２ｄ・・・）で情報の送受信を行うシステムにおいて、
前記発信加入者（２０２ａ）からの受信した暗号化情報の復号化、または受信加入者に送信する情報の暗号化を行う暗号計算部（２０３）と、
前記暗号化情報を復号化するための共通秘密鍵（２０４）と、各加入者に対応した暗号化を行うための各加入者毎の個別公開鍵（２０５ａ，２０５ｂ，２０５ｃ，２０５ｄ・・・）とを格納した鍵格納部（２０６）とを有する暗号化情報中継装置。
【請求項２】　前記に加えて、発信端末から発信加入者固有の秘密鍵で電子署名された情報を受信したときに、当該署名を検証するメンバ判断部を備えていることを特徴とする請求項１記載の暗号化情報中継装置。
【請求項３】　前記に加えて、発信加入者から受信した情報に基づいて秘密性の程度を変更可能な同報方式判断部を備えていることを特徴とする請求項１記載の暗号化情報中継装置。
【請求項４】　前記請求項１に記載した暗号化情報中継装置に接続される加入者端末であって、自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵とを格納した鍵格納部を有していることを特徴とする加入者端末装置。
【請求項５】　発信加入者から加入者共通の公開鍵で暗号化された情報を受信した場合に、この情報を加入者共通の秘密鍵で復号化した後、当該情報を各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する暗号通信方法。
【請求項６】　前記情報は発信加入者の秘密鍵によって電子署名がなされていることを特徴とする請求項５記載の暗号通信方法。
【請求項７】　前記秘密鍵によって電子署名された暗号化情報を受信した場合に、自身が有する当該発信加入者の公開鍵で前記電子署名を検証し、当該加入者が正規の加入者であるか否かを判定することを特徴とする請求項５記載の暗号通信方法。
【請求項８】　前記判定結果を前記発信加入者からの情報に添付して受信加入者に送信することを特徴とする請求項７記載の暗号通信方法。
【請求項９】　各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する際に、加入者共通の秘密鍵で電子署名することを特徴とする請求項５記載の暗号通信方法。
【請求項１０】　前記発信加入者は情報を暗号化することなく発信加入者が保有する秘密鍵によって情報に電子署名を行い前記暗号化情報中継装置に送信し、これを受信した前記暗号化情報中継装置は自身が保有している当該発信加入者の公開鍵を用いて電子署名を検証した後、加入者共通の秘密鍵で電子署名して各加入者に送信し、受信加入者はこの情報を受信した際に自身が保有している加入者共通の公開鍵で当該電子署名を検証することを特徴とする請求項５記載の暗号通信方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、計算機を相互に接続したネットワークにおいて、情報の同報通信時の際の機密保持に適用して有効な技術に関する。
【０００２】
【従来の技術】近年のネットワーク環境下では、情報交換・提供の手段として電子メールや電子掲示板等が多用され始めてきている。
【０００３】この種のネットワークでは開放的なアーキテクチャに基づいてシステムが構築されているため、いわゆる電子メールののぞき見や第三者への機密情報の漏洩等が常に問題となっていた。
【０００４】上記に加えて、オンラインショッピングやホームバンキング等のようにネットワーク利用を前提とした商用サービスが次々と実現していくなかで、予期しない第三者への機密情報の漏洩は犯罪を誘発する要因となりかねない。
【０００５】このような点に鑑みて、ネットワーク上でのセキュリティを高めるため、送り手はデータを暗号化してネットワーク上に送信し、受信側では受信した暗号化データを解読して基のデータ形式に戻すという、いわゆる暗号通信システムが種々研究されている。
【０００６】同報通信（単一の送り手から複数の受け手に情報を送信する方式）において用いられている暗号通信方式としては下記のものがある。
〔共通鍵方式〕「共通鍵方式」は、メンバ（発信者および受信者）が共通の公開鍵（暗号化するための鍵）と秘密鍵（復号化するための鍵）とを共有する形態である。発信者は、このメンバ間で共通の公開鍵を用いて情報を暗号化して送信する。これを受け取った受信者は、メンバ共通の秘密鍵で暗号化情報を復号（平文化）してその情報を読みとる方式である。これを図９を用いてさらに説明する。
【０００７】同図は、情報１００を送信側のメンンバ（暗号装置Ａ１）から、受信側の各メンバ（暗号装置Ｂ１，Ｃ１，Ｄ１）に対して同報通信する場合を説明している。送信側の暗号装置Ａ１の記憶部１０４内には、メンバ共通の公開鍵Ｏ１と、秘密鍵Ｓ１とが用意されている。暗号装置Ａ１は、まず情報１００を前記公開鍵Ｏ１で暗号化して送信する。そして同報通信された暗号化情報１０１，１０１，１０１を受け取った受信者側の暗号装置Ｂ１，Ｃ１，Ｄ１は、それぞれの記憶部１０４ａ，１０４ｂ，１０４ｃ内に用意している秘密鍵Ｓ１，Ｓ１，Ｓ１を用いて当該暗号化情報１０１，１０１，１０１を復号化して平文（１０２、１０２、１０２）とす

る。ここで平文とは人間または機械で可読な情報を指す。

〔個別鍵方式〕「個別鍵方式」では、各メンバがメンバのリストと全てのメンバの公開鍵のリストを共有する形態である。

【０００８】発信者は、情報を各メンバ（受信者）の公開鍵で暗号化して送信する。これを受け取った受信者は、自身の秘密鍵で暗号化情報を復号化してその情報を読みとる。

【０００９】この個別鍵方式を図１０を用いて説明する。同図に示すように、送信側の記憶部１０７ａには自身が受け取った暗号化情報を復号化するための秘密鍵ＳＡとともに、各メンバの公開鍵ＯＡ，ＯＢ，ＯＣ，ＯＤが保持されている。同様に、受信側の暗号装置Ｂ２，Ｃ２，Ｄ２の記憶部（１０７ｂ，１０７ｃ，１０７ｄ）内においても自身の秘密鍵（ＳＢ，ＳＣ，ＳＤ）とともに各メンバの公開鍵（ＯＡ～ＯＤ）がそれぞれ保持されている。

【００１０】ここで、Ａ２より情報１０５を各メンバ（Ｂ２，Ｃ２，Ｄ２）に送信する場合、まずメンバＢ２の公開鍵Ｏ２を用いて暗号化した情報（暗号化情報１０５ｂ）を作成し、同様にメンバＣ２の公開鍵ＯＣを用いて暗号化情報１０５ｃを作成し、メンバＤ２の公開鍵ＯＤを用いて暗号化情報を１０５ｄを作成した後、それぞれのメンバＢ２，Ｃ２，Ｄ２に送信する。

【００１１】これらの暗号化情報を受信した各メンバＢ２，Ｃ２，Ｄ２ではそれぞれの秘密鍵ＳＢ，ＳＣ，ＳＤを用いて平文化する（１０６ｂ，１０６ｃ，１０６ｄ）。

【００１２】

【発明が解決しようとする課題】ところが、上記従来技術では下記のような問題があった。

【００１３】〔共通鍵方式の問題点〕メンバ共通の秘密鍵（Ｓ１）を、メンバ全員で管理するため、第三者に秘密鍵を知得されてしまう可能性が高く秘密漏洩を生じやすい。また、悪意を有するメンバが意図的に秘密鍵を横流しする不法行為も否定できなかった。

【００１４】また、メンバがこの同報通信システムから脱会するときには情報漏洩防止のために、新たに残存メンバ共通の秘密鍵を再作成して残存メンバに配布しなおさなければならず、同報通信システムの加入者が増加してくるとその管理が煩雑になる恐れがあった。

【００１５】さらに、公開鍵が公開されることにより、予期しない第三者がこの同報通信システムに情報を送信することができるようになり、特定者間の情報流通の閉鎖性が損なわれてしまう可能性があった。

【００１６】〔個別鍵方式の問題点〕各メンバが全メンバのリストと公開鍵を管理しなければ、各メンバの暗号装置における記憶部の負担が増大する恐れがあった。

【００１７】また、メンバが同報通信システムに加入・脱退するときには残存メンバが各々保持している加入者・脱退者の公開鍵の情報を更新させなくてはならず、同報通信システムの加入者が増減した場合にはその管理・維持が非常に煩雑になる可能性があった。

【００１８】さらに、上記において各メンバが遠隔地に分散している場合、更新情報の伝達に時間がかかり、残存メンバ間の情報に矛盾を生じ、システムの円滑な運用が困難になる可能性もあった。

【００１９】本発明は、前記課題に鑑みてなされたものであり、各メンバが管理しなければならない秘密情報を最小限に抑制し、メンバの加入・脱退にも柔軟に対応できる同報暗号通信システムを提供するものである。

【００２０】

【課題を解決するための手段】本発明の第１の手段は、図１に示すように、通信回線２０１で接続された複数の加入者間２０２ａ，２０２ｂ，２０２ｃ，２０２ｄで情報の送受信を行うシステムであって、前記発信加入者２０２ａからの受信した暗号化情報の復号化、または受信加入者に送信する情報の暗号化を行う暗号計算部２０６と、前記復号化するための共通秘密鍵２０４と、各加入者に対応した暗号化を行うための各加入者毎の個別公開鍵２０５ａ，２０５ｂ，２０５ｃ，２０５ｄとを格納した鍵格納部２０６とを有する暗号化情報中継装置としたものである。

【００２１】第２の手段は、前記に加えて、発信端末から発信加入者固有の秘密鍵で電子署名された情報を受信したときに、当該署名を検証するメンバ判断部を備えるようにしたものである。

【００２２】第３の手段は、前記に加えて、発信加入者から受信した情報に基づいて秘密性の程度を変更可能な同報方式判断部を備えたものである。第４の手段は、前記暗号化情報中継装置に接続される加入者端末について、自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵とを格納した鍵格納部を有するものである。

【００２３】第５の手段は、発信加入者から加入者共通の公開鍵で暗号化された情報を受信した場合に、この情報を加入者共通の秘密鍵で復号化した後、当該情報を各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信するようにした。

【００２４】第６の手段は、前記第５の手段において前記情報に対して発信加入者の秘密鍵によって電子署名するようにした。第７の手段は、前記第５の手段において、前記秘密鍵によって電子署名された暗号化情報を受信した場合に、自身が有する当該発信加入者の公開鍵によって電子署名を検証し、当該加入者が正規の加入者であるか否かを判定するようにした。

【００２５】第８の手段は、前記第７の手段において、前記判定結果を前記発信加入者からの情報に添付して受信加入者に送信するようにした。第９の手段は、前記第

５の手段において、各加入者毎の個別公開鍵で暗号化して対応する受信加入者に送信する際に、加入者共通の秘密鍵で電子署名するようにした。

【００２６】第１０の手段は、前記第５の手段において、前記発信加入者は情報を暗号化することなく発信加入者が保有する秘密鍵によって情報に電子署名を行い前記暗号化情報中継装置に送信し、これを受信した前記暗号化情報中継装置は自身が保有している当該発信加入者の公開鍵を用いて当該電子署名を検証した後、加入者共通の秘密鍵で電子署名して各加入者に送信し、受信加入者はこの情報を受信した際に自身が保有している加入者共通の公開鍵で当該電子署名を検証する暗号通信方法である。

【００２７】

【作用】前記第１の手段によれば、暗号化情報中継装置を介在させることにより、この暗号化情報中継装置が暗号鍵の管理センターとして機能することにより、各加入者が共通の秘密鍵を共有することなく、機密の漏洩防止を効果的に実現できる。また加入者の脱退や新規加入の場合には、この暗号化情報中継装置に集中されたデータベースを更新するのみで良いため、加入者が増加した場合にもこれらの管理が煩雑にはならない。

【００２８】第２の手段によれば、情報の送信に際して、発信加入者に加入者自身しか知らない個別秘密鍵で電子署名させることにより、暗号化情報中継装置では当該情報が正規の加入者から送られてきたものか否かを判別することができる。そのため、正規加入者以外の送信者からの情報を特定することができる。

【００２９】第３の手段によれば、同報方式判断部を備えることにより、暗号化情報中継装置から送信する情報の秘密性の度合いを変更できる。したがってネットワークの状態に応じて必要以上の秘密化処理を行うことなく常に最適な秘密処理を選択できる。

【００３０】第４の手段によれば、加入者端末として自身が送信する情報を暗号化するための共通公開鍵と、自身が受信した情報を復号化するための個別秘密鍵のみを保持すればよいため、各加入者が必要以上の秘密情報を管理することがなく、機密性を高めることができる。

【００３１】第５の手段によれば、前記第１の手段同様、各加入者の共有する秘密情報（共通秘密鍵など）を最小限にすることができるため、機密の漏洩を効果的に防止できるとともに、加入者の増加にも柔軟に対応できる。

【００３２】第６および第７の手段によれば、電子署名により送信加入者の正規性の判定を容易に行うことができ、たとえば脱退した元加入者が正規加入者になりすまして残存加入者に秘密情報を送信することを容易にチェックできる。

【００３３】第８の手段によれば、受信側加入者は前記暗号化情報中継装置による判定結果を情報とともに受け取ることにより、判定結果を参照して自身が読む必要のある情報か否かを判断することが容易となる。

【００３４】第９の手段によれば、前記暗号化情報中継装置が加入者共通の秘密鍵で電子署名して情報を送ることにより、第三者が中継装置になりすまして情報を送信することを防止でき、前記暗号化情報中継装置と受信加入者との間の通信機密性をさらに高めることができる。

【００３５】第１０の手段によれば、情報を暗号化しなくても電子署名の検証により発信加入者の正当性を検証できる。要するに本発明によれば、暗号化して情報中継を行うことにより第三者による情報の盗聴を防止することができ、また電子署名した情報を中継することにより第三者が正当な発信者になりすますことを検出・防止できる。

【００３６】

【実施例１】図２は、本発明の実施例１のシステム構成を示している。本実施例では、暗号通信の手段として、ＰＥＭ（Privacy Enhanced Mail）を用いる。ＰＥＭは、インターネット（Internet)における標準化文書rfc 1421-1242に規定されている暗号電子メールの標準形式であり、情報を秘密鍵暗号ＤＥＳで暗号化し、その鍵を公開暗号ＲＳＡ（後述する）を用いて暗号化し送信するものである。

【００３７】同図において、暗号化情報中継装置１は、通信回線２によって加入者端末装置Ａ３，Ｂ３，Ｃ３とそれぞれ接続されている。本実施例では説明の便宜上、加入者Ａ３（加入者端末Ａ３）から３名の加入者Ｂ３，Ｃ３，Ｄ３（加入者端末Ｂ３，Ｃ３，Ｄ３）に暗号化情報を同報通信する場合で説明するが実際の秘密情報通信ではさらに多くの加入者への同報通信が必要であることはいうまでもない。

【００３８】各加入者端末装置Ａ３，Ｂ３，Ｃ３，Ｄ３にはそれぞれ鍵格納部３ａ，３ｂ，３ｃ，３ｄが設けられており、この鍵格納部内には共通の公開鍵ＯＭ１と各個々の端末（加入者）の公開鍵と秘密鍵の対（ＯＡ１とＳＡ１，ＯＢ３とＳＢ３，ＯＣ３とＳＣ３，ＯＤ３とＳＤ３）が登録されている。

【００３９】暗号化情報中継装置１の鍵格納部４内には、共通公開鍵ＯＭ１と共通の秘密鍵ＳＭ１および各加入者の公開鍵ＯＡ２，ＯＢ２，ＯＣ２，ＯＤ２が登録されている。

【００４０】ここで、「公開鍵」とは情報を暗号化するためのものであり、「秘密鍵」は暗号化された情報を復号化するものである。このような公開鍵と秘密鍵を用いた暗号方式としては、ＲＳＡ（R.L.Rivest, A.Shamir, L.Adleman）が知られている。このＲＳＡについて簡単に説明する。ＲＳＡが使用する数論特性は「ｎに対して互いに素であるｉをφ（ｎ）乗し、modｎを掛けると１になる」という点である。これは次の式で表される。

【００４１】

【数１】 $i\phi^{(n)} \pmod n = 1$
ｅおよびｄをモジェロφ（ｎ）の逆数であるランダムは整数と仮定する。これを式で表すと次式のようになる。
【００４２】
【数２】ｅｄ＝１（modφ（ｎ））
オイラーの定理では、Ｍがｎに対して互いに素であるとき、次の二つの関係が成り立つ。
【００４３】
【数３】$(M^e)^d = M \pmod n$
$(M^d)^e = M \pmod n$
これを暗号法に適用すると、Ｍがメッセージ（情報）の一部であるとき、次の関数でメッセージをコード化できる
【００４４】
【数４】$s = M^e \pmod n$
一方復号するときには次の関数となる。
【００４５】
【数５】$M = s^d \pmod n$
次に、オイラーのファイ関数φ（ｐｑ）を計算する。ｎを２つの素数の積とすると、φ（ｐｑ）＝（ｐ－１）（ｑ－１）＝φ（ｎ）という式が成り立つ。
【００４６】次に、φ（ｎ）に対して互いに素である値ｅを選択する。このとき、max（ｐ＋１，ｑ＋１）＜ｅ＜φ（ｎ）の範囲にある値を選択するとよい。さらに（ｅｄ）＝１（modφ（ｎ））となるような値ｄを計算する。すなわちφ（ｎ）を法としたｅの逆数を求めるのである。ｄの値が小さすぎたときには（$\log_2 n$未満）、ｅおよびｄの値を変える。
【００４７】メッセージｍを暗号化するにはｍをｎより小さい固定サイズの整数Ｍに分割する。次にメッセージの各部分について（M^e）（modｎ）＝ｓの値（これが公開鍵となる）を求める（本実施例では暗号計算部６が行う）。これらの値が連結されて暗号化情報が生成される（連結処理は情報作成部７で行ってもよい）。
【００４８】このメッセージ（暗号化情報）を復号化するには、メッセージをブロックに分割し各ブロックを（s^d）（modｎ）＝Ｍ（これが秘密鍵となる）で復号する。各加入者端末装置Ａ３の内部構成をさらに詳しく示したものが図３である。同図において、共通公開鍵ＡＭ１、個別公開鍵ＯＡ１および個別秘密鍵ＳＡ１が格納されている鍵格納部３ａは暗号計算部６からアクセスされる。情報作成部７は文書を作成するエディタ等を備えている。また通信インターフェース８は通信回線２との通信手順を実行する。これらの暗号計算部６，情報作成部７および通信インターフェース８は制御部５により制御される。これらの各部は具体的にはコンピュータシステムを用いて実現されており、鍵格納部３ａは磁気記録媒体上に生成され、暗号計算部６は所定のロジックを制御部のプロセッサが実行することで実現されている。
【００４９】図４は、本実施例における暗号化情報中継装置１の内部構成をさらに詳しく説明したものである。同図に示すように、鍵格納部１１には共通公開鍵ＯＭ１およびこれに対応する秘密鍵ＳＭ１、そして各加入者の公開鍵ＯＡ２，ＯＢ２・・・・が格納されている。
【００５０】この鍵格納部１１は、インデックスとして機能するメンバ情報格納部１４を有しており、このメンバ情報格納部１４には加入者の情報これに対応づけられた加入者の公開鍵とが登録されている。当該暗号化情報通信システムの管理者は、制御部１２を通じてこのメンバ情報格納部１４を修正・削除・追加することにより鍵格納部１１を更新することができる。
【００５１】鍵格納部１１は、暗号計算部６からアクセスされ秘密鍵および公開鍵が読み出されるようになっている。メンバ判断部１３は、発信端末からの情報に付された電子署名を解析して当該発信者が正当な加入者であるか否かを検証する。
【００５２】通信インターフェースは、通信回線２との通信手順を実行する。これらの暗号計算部６，メンバ判断部１３および通信インターフェース８は制御部１２により制御される。これらの各部は具体的にはコンピュータシステムを用いて実現されており、鍵格納部１１およびメンバ情報格納部１４は磁気記録媒体上に生成され、暗号計算部６は所定のロジックを制御部１２のプロセッサが実行することでその機能が実現されている。
【００５３】次に以上に説明した図２～図４に基づいて、加入者端末Ａ３から情報を暗号化して暗号化情報中継装置１を経由して各端末Ｂ３，Ｃ３，Ｄ３に配信する場合について説明する。
【００５４】加入者発信端末Ａ３では、情報をまず共通の公開鍵ＯＭ１で暗号化して暗号化情報を生成し、通信回線２上に送信する。当該暗号化情報を受信した暗号化情報中継装置１では、秘密鍵ＳＭ１でこの暗号化情報を平文化（人間または機械が可読な情報形式にすること）する。
【００５５】次に、暗号化情報中継装置１は、加入者端末Ｂ３の公開鍵ＯＢ２を用いて前記平文化された情報を再度暗号化する。このようにして再暗号化された情報は、通信回線２上に送信される。これを受信した受信加入者端末Ｂ３では、自身の秘密鍵ＳＢ３を用いて前記再暗号化情報を平文化する。
【００５６】前記再暗号化の際に、暗号化情報中継装置１では、公開鍵ＯＣ２およびＯＤ２を用いて前記と同様に情報を再暗号化してそれぞれの加入者受信端末Ｃ３，Ｄ３に送信する。これを受信した各受信加入者端末Ｃ３，Ｄ３では、自身の秘密鍵ＳＣ３，ＳＤ３を用いて前記再暗号化情報を平文化する。
【００５７】このように、本実施例によれば各加入者の公開鍵の情報は暗号化情報中継装置１が集中管理しており、各加入者が管理しているのは共通公開鍵ＯＭ１と各自の公開鍵と秘密鍵の組み合わせのみである。したがっ

て、各加入者が加入者共通の秘密鍵を管理する必要がなく、加入者の脱退・新規加入の場合には暗号化情報中継装置１のデータを書き換えるだけでよく、同報暗号通信システムの管理者のみでこれらの脱退・新規加入に迅速に対応できる。したがって、脱退・加入にともなって残存加入者に対して加入者共通の公開鍵および秘密鍵を再度設定しなくてもよい。

【００５８】

【実施例２】図５は本発明の実施例２のシステム構成を示すブロック図である。本実施例２のシステム構成は前記実施例１で説明した図２とほぼ同様であるが、暗号化情報に電子署名がなされている点が異なる。

【００５９】本実施例において発信加入者端末Ａ３から暗号化情報中継装置１を経由して受信加入者端末Ｂ３，Ｃ３，Ｄ３に送信する場合について以下に説明する。発信加入者端末では、発信加入者端末Ａ３の情報作成部７（図３参照）によって情報を作成する。

【００６０】次に、暗号計算部６によって、加入者共通の公開鍵ＯＭ１を用いて前記情報を暗号化する。次に発信加入者端末は、暗号計算部６によって前記暗号化情報に対して自身の秘密鍵ＳＡ１によって電子署名を行う。

【００６１】このようにして生成された暗号化情報と電子署名とを通信インターフェース８を通じて通信回線２上に送信する。このとき、発信加入端末Ａ３は、同報通信の受信側電子メールのアドレスを指定する。

【００６２】電子メールシステム２２２では、暗号化情報と電子署名とをメールアドレスに従って暗号化情報中継装置１に送信する。暗号化情報中継装置１が通信インターフェース８を通じて前記暗号化情報と電子署名とを受信すると、制御部１２の制御により暗号計算部６を通じて加入者共通の秘密鍵ＳＭ１を用いて当該暗号化情報を平文化した後、前記電子署名を検証する。この検証は、具体的には鍵格納部１１に登録された発信加入者の公開鍵ＯＡ２を用いることによって前記電子署名の正当性を確認できる。

【００６３】次に、メンバ判断部は、メンバ情報格納部１４を参照して、発信者の電子メールアドレスを用いて、送信者が正規の加入者であるか否かを判定する。次に、制御部１３は暗号計算部６を制御して、前記情報に対して加入者共通の秘密鍵ＳＭ１によって電子署名する。

【００６４】次に制御部１２は、暗号計算部６を制御して情報を各加入者の公開鍵で暗号化して暗号化情報を生成する。たとえば加入者端末Ｂ３に送信する情報であれば公開鍵ＯＢ２を用いて暗号化し、加入者端末Ｃ３に送信する情報であれば公開鍵おＣ３を用いて暗号化する。

【００６５】次に暗号化情報中継装置１は、前記で再暗号化された情報と電子署名とを通信インターフェース８を通じて電子メールシステム２２２に送信する。電子メールシステム２２２では、暗号化情報と電子署名とを各加入者のメールアドレスに従って各加入者に送信する。

【００６６】前記暗号化情報と電子署名とを受信した加入者（たとえば加入者端末Ｂ３）は、自身の制御部５を通じて暗号計算部６によって各自の秘密鍵（たとえばＳＢ３）を用いて前記暗号化情報を復号する。

【００６７】次に受信側加入者端末Ｂ３は、暗号計算部６を通じて加入者共通の公開鍵ＯＭ１を用いて前記電子署名を検証する。このように本実施例によれば、電子署名を用いることにより、発信者が自分の身元を保証する手段を実現し、また暗号化情報中継装置１が加入者になりすますことを防止できる。すなわち、受信加入者としては電子署名を検証することにより、発信者が非合法であるか否か、つまり第三者が暗号化情報中継装置１になりすましているか否かを容易に確認することができる。

【００６８】

【実施例３】図６は本発明の実施例３のシステム構成を示すブロック図である。本実施例３のシステム構成は前記実施例２で説明した図５とほぼ同様であるが、暗号化を行わずに電子署名のみで平文情報を通信する点が特徴である。

【００６９】本実施例において発信加入者端末Ａ３から暗号化情報中継装置１を経由して受信加入者端末Ｂ３，Ｃ３，Ｄ３に送信する場合について以下に説明する。なお、加入者端末の構成および暗号化情報中継装置１の構成については先に説明した図３および図４を用いる。

【００７０】発信加入者端末Ａ３では、制御部５の制御情報作成部７によって送信すべき情報を作成する。次に制御部５の制御により暗号計算部６を通じて当該情報に対して発信加入者の秘密鍵ＳＡ１を用いて電子署名する。

【００７１】発信加入端末は、前記情報と電子署名とを通信インターフェース８を通じて電子メールシステム２２２に送信する。電子メールシステム２２２は、電子メールアドレスにしたがって、前記情報と電子署名とを暗号化情報中継装置１に送信する。

【００７２】前記情報と電子署名とを受信した暗号化情報中継装置１では、暗号計算部６を通じて当該電子署名を検証する。そして、メンバ判断部１３によってメンバ情報格納部１４を参照し、発信者のメールアドレスに基づいて当該発信者が正規の加入者であるか否かを判定する。

【００７３】次に制御部１２の制御により暗号計算部６を通じて当該情報を加入者共通の秘密鍵ＳＭ１を用いて電子署名する。このようにして得られた情報と電子署名と制御部１２はを通信インターフェース８を通じて電子メールシステム２２２に送信する。

【００７４】電子メールシステム２２２を経由して前記情報と電子署名とを受信した加入者端末（たとえばＢ３）は、自身の暗号計算部６を通じて加入者共通の公開鍵ＯＭ１を用いて前記電子署名を検証する。

【００７５】このように本実施例によれば、暗号化を行うことなく平文のまま情報を送信する場合にも、電子署名を用いることにより、発信者が自分の身元を保証する手段を実現できており、受信加入者としては電子署名を検証することにより、発信者が非合法であるか否かを容易に確認することができ、不要な情報を読む前に拒絶することができる。

【００７６】

【実施例４】図７は、本発明の実施例４における暗号化情報中継装置２１を示している。本実施例の暗号化情報中継装置２１は、前述の実施例１で説明した暗号化情報中継装置１の構成とほぼ同様であるが、同報方式判断部２２が設けられている点が特徴である。

【００７７】なお、全体のシステム構成については図２と同様であるので説明の便宜上図２を用いる。前記同報方式判断部２２のさらに詳しい構成を示したものが図８である。同図において同報方式判断部２２は、発信者情報判断部２３，同報方式選択部２４および同報方式指示部２５で構成されている。発信者情報判断部２３は、発信者からの情報がどのようなモードで送信されたかを判断するもので、発信加入者端末から暗号化情報中継装置２１に至る情報のモードとしては以下の２通りがある。

（１）情報と、この情報を発信者の秘密鍵で電子署名したもの

（２）情報を加入者共通の公開鍵で暗号化した暗号化情報と、情報を発信者の秘密鍵で署名したもの

上記（１）は情報が平文で送信された場合であり、

（２）は情報が暗号で送信された場合である。

【００７８】同報方式選択部２４は、当該暗号化情報中継装置２１より受信加入端末までの情報のモードを選択する機能を有している。このモードとしては以下の４通りがある。

（３）情報と、情報を加入者共通の秘密鍵で署名したもの

（４）情報を各加入者の公開鍵で暗号化した暗号化情報と、情報を加入者共通の秘密鍵で電子署名したもの

（５）発信者から送信されてきた情報の電子署名の検証結果を情報に添付した検証結果添付情報と、検証結果添付情報を加入者共通の秘密鍵で署名したもの

（６）発信者から送信されてきた情報の電子署名の検証結果を情報に添付した検証結果添付情報を、各加入者の公開鍵で暗号化したものと、検証結果添付情報を加入者共通の秘密鍵で電子署名したもの

同報方式選択部２４は、前記（１）と（３）～（６）との組み合わせ、または前記（２）と（３）～（６）との組み合わせによる合計８通りのモードを選択することが可能である。

【００７９】同報方式選択部２４による選択に際しては、当該システムの状態に応じて必要とする機密性のレベルを選べば良く、たとえば（１）と（３）の組み合わせによれば前述の実施例３に説明した平文情報に電子署名を伴う通信方式となり、最も高い機密性を要求する場合には（２）と（６）との組み合わせとなる。すなわち、（２）と（６）との組み合わせでは、暗号化情報と電子署名とを通信対象とし、暗号化情報中継装置２１で検証した電子署名の検証結果をも受信加入者端末に送信されるため、受信者は機密性の保証をより高く受けられることになる。

【００８０】以上の各実施例の説明では加入者端末の鍵格納部に加入者の公開鍵と秘密鍵とが登録されている例で説明したが、これらの端末における鍵格納部は固定的なものでなく、たとえば加入者は、ＩＣカード等の記録媒体に共通公開鍵と自身の公開鍵および秘密鍵を登録しておき、これを持参し、必要な場合に近くの汎用的な端末装置のＩＣカードスロットに当該ＩＣカードを装着することにより各実施例で説明したような当該加入者固有の加入者端末を実現するようにしてもよい。

【００８１】また以上の各実施例の説明では、暗号通信方式としてＰＥＭを用いたが、他の通信方式であってもよいことは勿論である。また暗号方式としてもＲＳＡに限られない。

【００８２】

【発明の効果】本発明によれば、同報暗号通信において、各メンバが管理しなければならない秘密情報を最小限に抑制し、メンバの加入・脱退にも柔軟に対応できる。

【図面の簡単な説明】

【図１】本発明の原理図

【図２】本発明の実施例１におけるシステム構成を示すブロック図

【図３】実施例１において加入者端末装置の内部構成を示すブロック図

【図４】実施例１における暗号化情報中継装置の内部構成を示すブロック図

【図５】本発明の実施例２のシステム構成を示すブロック図

【図６】本発明の実施例３のシステム構成を示すブロック図

【図７】本発明の実施例４における暗号化情報中継装置２１の構成を示すブロック図

【図８】実施例４における同報方式判断部の構成を示すブロック図

【図９】共通鍵方式を説明するためのシステム構成図

【図１０】個別鍵方式を説明するためのシステム構成図

【符号の説明】

１００・・情報

Ａ３，Ｂ３，Ｃ３・・加入者端末

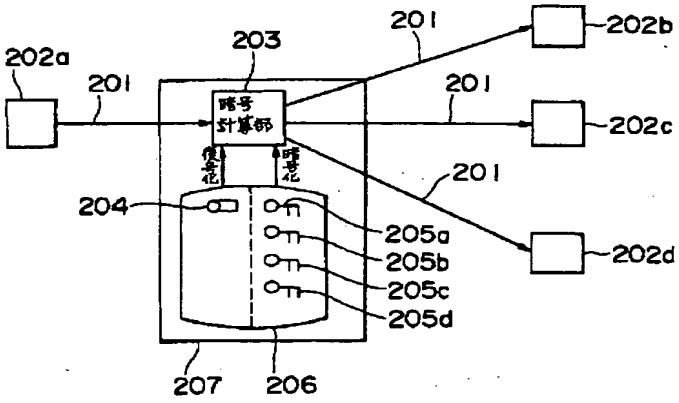
１・・暗号化情報中継装置

２・・通信回線

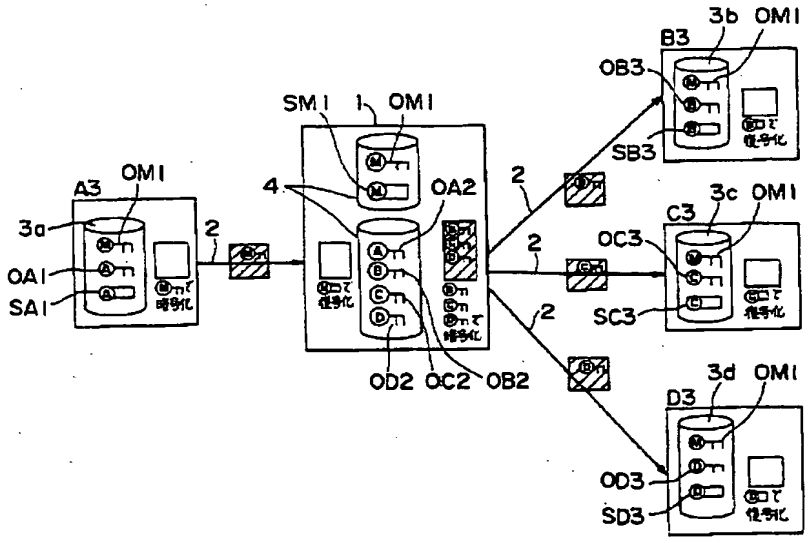
３ａ・・鍵格納部

５・・制御部
６・・暗号計算部
７・・情報作成部
８・・通信インターフェース
１１・・鍵格納部
１３・・メンバ判断部
１４・・メンバ情報格納部
２１・・暗号化情報中継装置
２２・・同報方式判断部
２０１・・通信回線
２０２ａ，２０２ｂ，２０２ｃ，２０２ｄ・・加入者（加入者端末）
２０３・・暗号計算部
２０４・・共通秘密鍵
２０５ａ，２０５ｂ，２０５ｃ，２０５ｄ・・個別公開鍵
２０６・・鍵格納部
２２２・・電子メールシステム

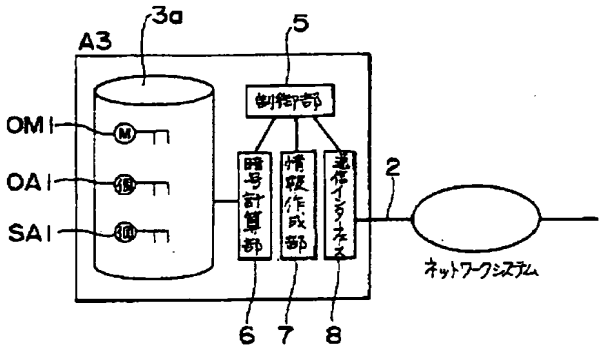
【図１】



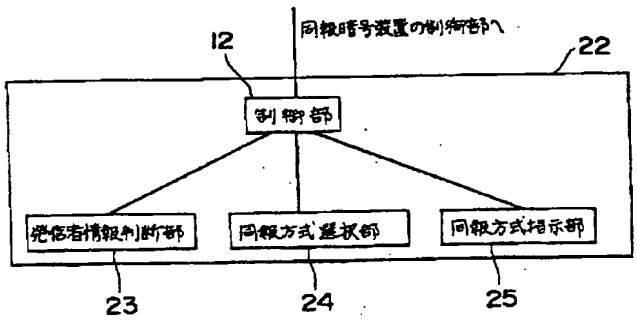
【図２】



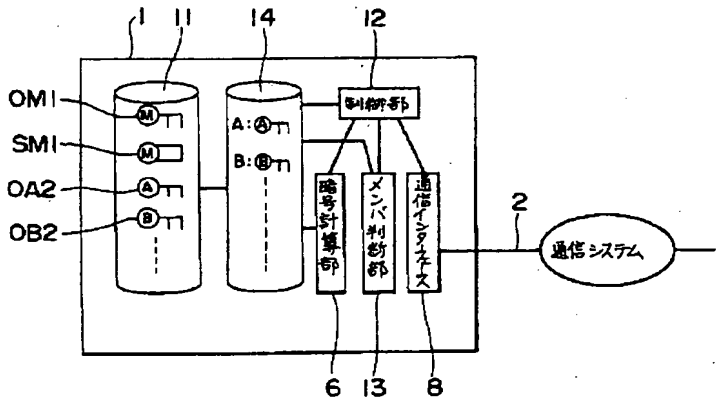
【図３】


A3
3a
5
制御部
OM1
OA1
SA1
暗号計算部
情報作成部
通信インターフェース
2
ネットワークシステム
6
7
8

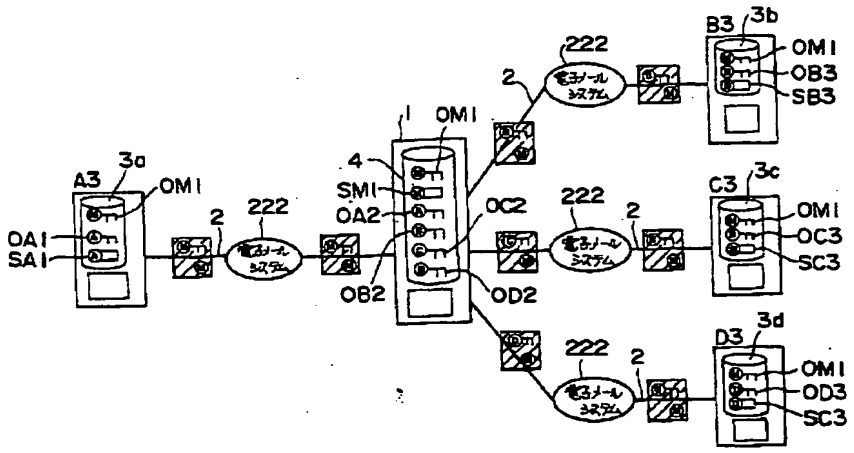
【図８】


同報暗号装置の制御部へ
12
22
制御部
発信者情報判断部
同報方式選択部
同報方式指示部
23
24
25

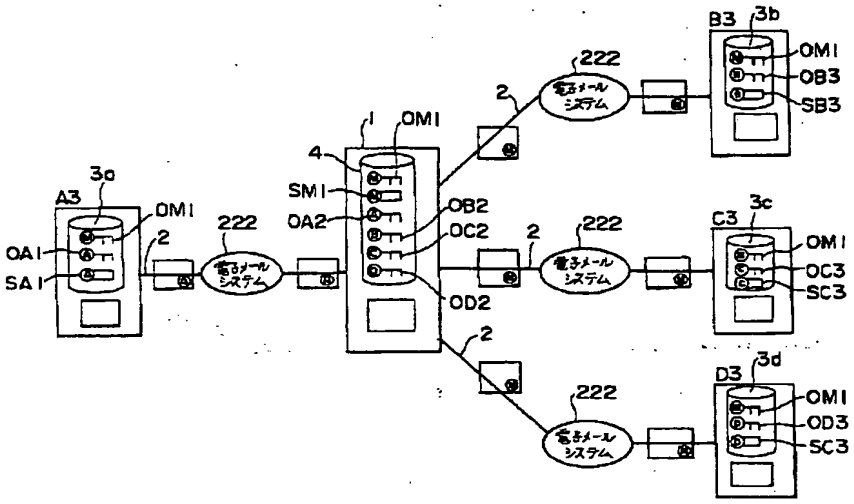
【図４】


1
11
14
12
OM1
SM1
OA2
OB2
A:Ⓐ
B:Ⓑ
制御部
暗号計算部
メンバ判断部
通信インターフェース
2
通信システム
6
13
8

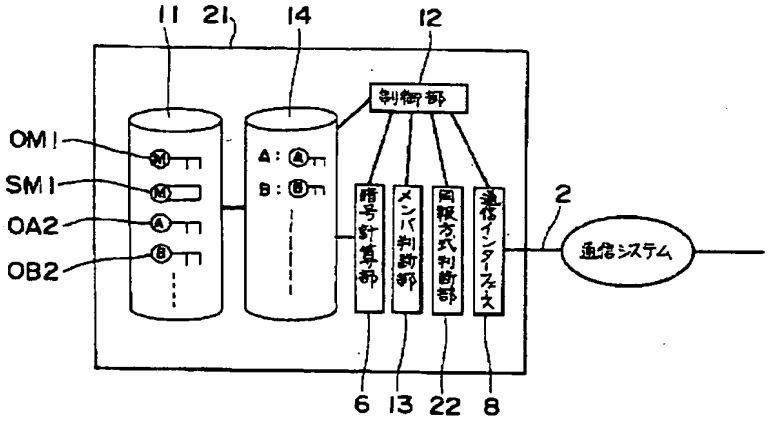
【図５】


A3
3a
OM1
OA1
SA1
2
222
電子メールシステム
1
OM1
4
SM1
OA2
OB2
OC2
OD2
B3
3b
OM1
OB3
SB3
C3
3c
OM1
OC3
SC3
D3
3d
OM1
OD3
SC3

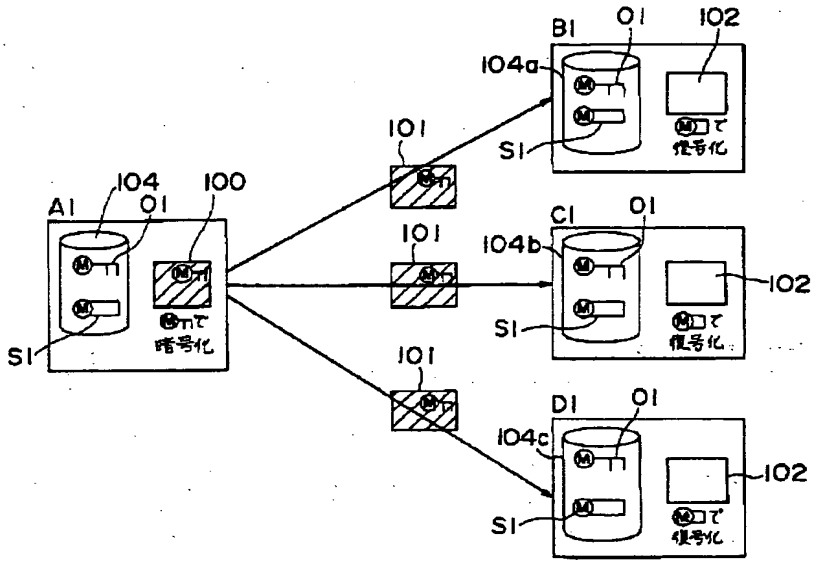
【図６】


B3
3b
OM1
OB3
SB3
222
電子メールシステム
2
1
OM1
4
SM1
OA2
OB2
OC2
OD2
3a
A3
OM1
OA1
SA1
C3
3c
OC3
SC3
D3
3d
OD3

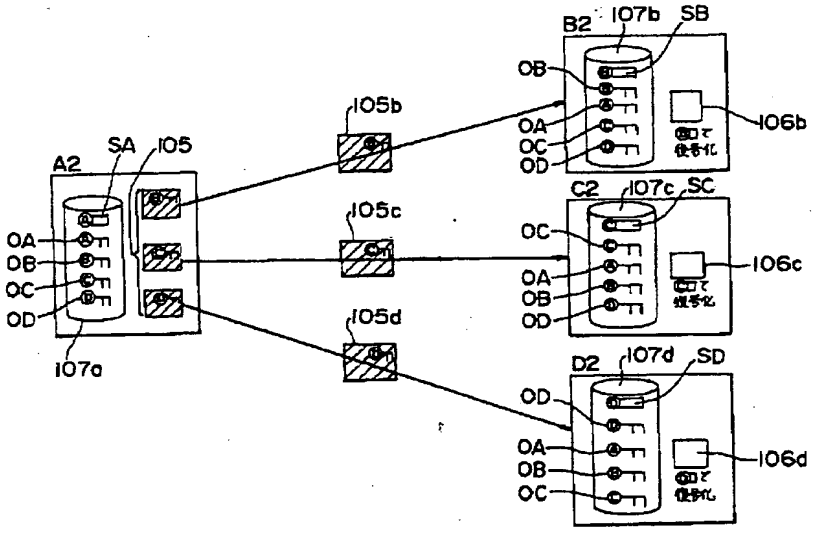
【図７】


11
21
14
12
制御部
OM1
SM1
OA2
OB2
A : A
B : B
暗号計算部
メンバ判断部
同報方式判断部
通信インターフェース
2
通信システム
6
13
22
8

【図９】


A1
01
104
100
S1
暗号化
101
101
101
B1
01
102
104a
S1
復号化
C1
01
104b
S1
102
復号化
D1
01
104c
S1
102
復号化

【図１０】


A2
SA
105
OA
OB
OC
OD
107a
105b
105c
105d
B2
107b
SB
OB
OA
OC
OD
106b
C2
107c
SC
OC
OA
OB
OD
106c
D2
107d
SD
OD
OA
OB
OC
106d